FLAT-CONTAINING AND SHIFT-BLOCKING SETS IN $\mathbb{F}_2^r$

AART BLOKHUIS AND VSEVOLOD F. LEV

Abstract. For non-negative integers $r \ge d$, how small can a subset $C \subseteq \mathbb{F}_2^r$ be, given that for any $v \in \mathbb{F}_2^r$ there is a d-flat passing through v and contained in $C \cup \{v\}$? Equivalently, how large can a subset $B \subseteq \mathbb{F}_2^r$ be, given that for any $v \in \mathbb{F}_2^r$ there is a linear d-subspace not blocked non-trivially by the translate $B + v$? A number of lower and upper bounds are obtained.

1. Introduction

The well-known finite-field version of the Kakeya problem is to estimate the smallest size of a subset of a finite vector space, containing a line in every direction. A natural dual problem is to estimate the smallest size of a subset containing a line *through every point* of the space, with the possible exception of the point itself. (The problem would become trivial had we not excluded the anchor point from consideration. This can be considered as an analogue of forbidding the zero difference in the definition of a progression-free set.) More generally, given an integer d one can consider sets "essentially containing" a *d-flat* through every point of the space. This motivates the following definitions.

Let V be a finite vector space and d an integer with $0 \le d \le \dim V$. We say that a subset $C \subseteq V$ is *d-complete* if for every $v \in V$ there exists a d-subspace $L_v \le V$ such that

$$v + (L_v \setminus \{0\}) \subseteq C;$$

that is, through every point of V passes a d-flat entirely contained in C, save, perhaps, for the point itself. Equivalently, $C \subseteq V$ is d-complete if any translate of C contains all non-zero vectors of some d-subspace. By $\gamma_V(d)$ we denote the smallest possible size of a d-complete subset $C \subseteq V$; alternatively, $\gamma_V(d)$ is the smallest possible size of a union of the form

$$\bigcup_{v \in V} \big(v + (L_v \setminus \{0\})\big),$$

for all families $\{L_v \colon v \in V\}$ of d-subspaces.

Clearly, a subset $C \subseteq V$ is d-complete if and only if its complement $B := V \setminus C$ has the property that for every $v \in V$ there is a d-subspace $L_v \le V$ with

$$\big(v + (L_v \setminus \{0\})\big) \cap B = \varnothing.$$

We call sets with this property *non-blocking*; quantitatively speaking, $B \subseteq V$ is d-non-blocking if through every point of V passes a co-d-flat disjoint with B, with the possible exception of the point itself. Equivalently, $B \subseteq V$ is d-non-blocking if for any translate of B there is a co-d-subspace of V, avoiding all non-zero points of the translate. We denote by $\beta_V(d)$ the largest possible size of a d-non-blocking subset $B \subseteq V$.

The significance of the quantity $\beta_V(d)$ lies in the fact that every subset $B \subseteq V$ of size $|B| > \beta_V(d)$ is guaranteed to have a translate blocking (that is, having non-zero and non-empty intersection with) all co-d-subspaces of V.

Writing $r := \dim V$, from the discussion above we have

$$\beta_V(d) = |V| - \gamma_V(r-d) \tag{1}$$

for all $0 \le d \le r$. In view of this basic relation, our results can be equivalently stated in terms of either of the quantities γ_V and β_V. We do not follow any strong rule in this respect, each time choosing whatever seems more natural to us. In some cases, two restatements are given; in most other cases the result is stated in terms of γ_V if it is of primary interest for flats of low dimension, and in terms of β_V when it is mostly interesting for flats of low *co*-dimension.

It is straightforward to verify that for every finite vector space V of dimension $r := \dim V \ge 1$ we have

$$0 = \gamma_V(0) < \gamma_V(1) \le \cdots \le \gamma_V(r-1) < \gamma_V(r) = |V|; \tag{2}$$

equivalently,

$$0 = \beta_V(0) < \beta_V(1) \le \cdots \le \beta_V(r-1) < \beta_V(r) = |V|. \tag{3}$$

In what follows we confine ourselves to the situation where V is a vector space over the two-element field $\mathbb{F}_2$. We denote the r-dimensional vector space over this field by $\mathbb{F}_2^r$, and we abbreviate $\gamma_{\mathbb{F}_2^r}(d)$ as $\gamma_r(d)$, and $\beta_{\mathbb{F}_2^r}(d)$ as $\beta_r(d)$.

We present our results in three blocks. In Section 3 we make some basic observations and in particular, find $\gamma_r(1)$ and $\beta_r(1)$ (hence also $\gamma_r(r-1)$ and $\beta_r(r-1)$, cf. (1)), and determine $\gamma_r(2)$ up to a multiplicative factor; the very short proofs are also included in Section 3. Non-existence results showing that complete sets are large (and accordingly, non-blocking sets are small) are presented in Section 4. Section 5 lists a number of upper-bound estimates for γ_r (hence, lower-bound estimates for β_r), based on specific constructions of complete and non-blocking sets.

The proofs of the results discussed in Sections 4 and 5 are given in Sections 6 and 7, respectively.

2. Motivation and acknowledgement

Our initial motivation came from the following problem raised by Ernie Croot (personal communication with the second-named author). Suppose that to each $v \in \mathbb{F}_2^r$ there corresponds a subset $A_v \subseteq \mathbb{F}_2^r$, and write $2 \cdot A_v$ for the set of all non-zero elements of $\mathbb{F}_2^r$, representable as a sum of two elements of A_v. Given that all sets A_v are large, how large must the union $C := \cup_{v \in \mathbb{F}_2^r}(v + 2 \cdot A_v)$ be? Does there exist a constant $c > 1$ such that if $|A_v| > 2^r/r^c$, then C contains all but at most $2^r/r^c$ elements of $\mathbb{F}_2^r$? In the special case where all A_v are actually affine subspaces of $\mathbb{F}_2^r$, this question can be restated in our present terms: is it true that if $d < c \log_2 r$, then $\beta_r(d) < 2^r/r^c$? The reader will easily check that Theorem 4 below yields much stronger estimates: say, we have $\beta_r(d) < 2^{0.85r}$ whenever $d < 0.15r$. However, the general case where A_v are arbitrary sets (not necessarily affine subspaces) cannot be treated with our present approach.

We are grateful to Ernie Croot for bringing this problem to our attention.

3. Basic observations: lines, hyperplanes, and 2-flats

The quantities $\gamma_r(1)$ and $\beta_r(1)$ and, consequently, $\gamma_r(r-1)$ and $\beta_r(r-1)$, are easy to determine.

Theorem 1. *For every integer $r \geq 1$ we have $\gamma_r(1) = \beta_r(1) = 2$. Hence, $\beta_r(r-1) = \gamma_r(r-1) = 2^r - 2$.*

Proof. The equality $\gamma_r(1) = 2$ follows from the observation that a singleton set does not contain a 1-flat passing through its unique element, whereas for any two-element set $C \subseteq \mathbb{F}_2^r$ and any $v \in \mathbb{F}_2^r$, there is 1-flat passing through v and contained in $C \cup \{v\}$.

To find $\beta_r(1)$ we first notice that for any two-element set $B \subseteq \mathbb{F}_2^r$ there is a linear co-1-subspace, disjoint from $B \setminus \{0\}$; hence $\beta_r(1) \geq 2$. On the other hand, if $B = \{b_1, b_2, b_3\} \subseteq \mathbb{F}_2^r$ is a three-element set, then the translate $(b_1 + b_2 + b_3) + B = \{b_1 + b_2, b_2 + b_3, b_3 + b_1\}$ blocks every linear co-1-subspace: for, the vectors $b_1 + b_2$, $b_2 + b_3$, and $b_3 + b_1$ add up to 0, and therefore they are not simultaneously contained in the complement of a linear co-1-subspace. Thus, $\beta_r(1) \leq 2$, and it follows that, indeed, $\beta_r(1) = 2$. □

To estimate $\gamma_r(2)$ we remark that if every element of $\mathbb{F}_2^r$ is a sum of three pairwise distinct elements of a set $S \subseteq \mathbb{F}_2^r$, then $\binom{|S|}{3} \geq 2^r$, whence $|S| > \sqrt[3]{6} \cdot 2^{r/3}$. On the other hand, sets S of size $|S| = O(2^{r/3})$, with the property just mentioned, are known to exist: see, for instance, [CHLL97, Theorem 5.4.28], or consider a decomposition of $\mathbb{F}_2^r$ into the direct sum of three subspaces of roughly equal dimension and take S to be their union.

Theorem 2. *If $r \ge 2$, then $\gamma_r(2)$ is the smallest cardinality of a subset $C \subseteq \mathbb{F}_2^r$ with the property that every element of $\mathbb{F}_2^r$ is representable as a sum of three pairwise distinct elements from C. Consequently, $\gamma_r(2) = \Theta\bigl(2^{r/3}\bigr)$.*

Proof. Just notice that for given vectors $v, c_1, c_2, c_3 \in \mathbb{F}_2^r$ to form a 2-flat it is necessary and sufficient that $v = c_1 + c_2 + c_3$ and c_1, c_2, c_3 are pairwise distinct. □

An interesting property of the quantity $\gamma_r(d)$ is that for any fixed value of d, it is sub-multiplicative in r.

Lemma 1. *For any integer $r_1, r_2 \ge d \ge 0$ we have*

$$\gamma_{r_1+r_2}(d) \le \gamma_{r_1}(d)\gamma_{r_2}(d).$$

Proof. Let $r := r_1 + r_2$ and write $\mathbb{F}_2^r = V_1 \oplus V_2$, where $\dim V_1 = r_1$ and $\dim V_2 = r_2$. Find $C_1 \subseteq V_1$ and $C_2 \subseteq V_2$ such that for $i \in \{1, 2\}$ we have $|C_i| = \gamma_{r_i}(d)$ and C_i is d-complete in V_i. We claim that $C_1 + C_2$ is d-complete in $\mathbb{F}_2^r$, so that

$$\gamma_{r_1+r_2}(d) \le |C_1 + C_2| = |C_1||C_2| = \gamma_{r_1}(d)\gamma_{r_2}(d).$$

To see this, fix $v \in \mathbb{F}_2^r$, write $v = v_1 + v_2$ with $v_1 \in V_1$ and $v_2 \in V_2$, find d-flats $F_1 \subseteq V_1$ and $F_2 \subseteq V_2$ such that $v_i \in F_i \subseteq C_i \cup \{v_i\}$ for $i \in \{1, 2\}$, and select arbitrarily bases $\{e_1, \dots, e_d\}$ and $\{f_1, \dots, f_d\}$ of the linear d-spaces $v_1 + F_1$ and $v_2 + F_2$, respectively. Then all points of the d-flat $v + \langle e_1 + f_1, \dots, e_d + f_d\rangle$, other than v, are contained in $C_1 + C_2$. □

Using a standard argument, it is easy to derive from Lemma 1 that to any fixed $d \ge 1$ there corresponds some $\varkappa_d \in [0, 1]$ such that $\gamma_r(d) = 2^{(\varkappa_d + o(1))r}$ as $r \to \infty$. As it follows from Theorems 1 and 2, we have $\varkappa_1 = 0$ and $\varkappa_2 = 1/3$. For $d \ge 3$ the precise values of $\varkappa_d$ are not known to us, but we will see that $3/8 \le \varkappa_3 \le 3/7$ (Theorems 3 and 5), and that $\varkappa_d < 1/2$ for all d (Theorem 5).

4. Non-existence results: lower bounds for γ_r, upper bounds for β_r

By Theorem 2 and (2), we have $\gamma_r(3) = \Omega(2^{r/3})$. The following theorem presents an improvement of this estimate.

Theorem 3. *If $r \ge 15$ is an integer, then*

$$\gamma_r(3) > c \cdot 2^{3r/8},$$

where $c = (16464)^{1/8} \approx 3.3656$.

The argument employed in the proof of Theorem 3 (see Section 6) can also be used to estimate $\gamma_r(3)$ non-trivially for $3 \le r \le 14$; say, it is easy to derive from (11) that

$\gamma_r(3) > 2^{r/2}$ for every such r. The only reason to confine to $r \geq 15$ is that this allows us to keep the coefficient c reasonably large.

Corollary 1. *For integer $r \geq d \geq 3$, we have $\gamma_r(d) = \Omega(2^{3r/8})$ with an absolute implicit constant.*

Recall, that the entropy function is defined by

$$H(x) := -x \ln x - (1-x)\ln(1-x),\ 0 < x < 1,$$

and that

$$\frac{1}{\sqrt{2r}}\, e^{rH(d/r)} \leq \binom{r}{d} < \sum_{j=0}^{d} \binom{r}{j} \leq e^{rH(d/r)} \tag{4}$$

for all integer $1 \leq d \leq r/2$; this follows easily, for instance, from [McWS77, Ch. 10, §11, Lemmas 7 and 8]. (Although this is not used below, we remark that the expression in the right-hand side of (4) can be given a nice symmetrical form; namely, $e^{rH(d/r)} = r^r/(d^d(r-d)^{r-d})$.)

Using (4), it is easy to verify that our next theorem improves Corollary 1 for flats of dimension $d \gtrsim 0.073r$ (by which we mean $d > (\varkappa + o(1))r$ with an absolute constant $\varkappa \approx 0.073$).

Theorem 4. *For integer $r \geq d \geq 0$ we have*

$$\gamma_r(d) \geq \sum_{j=0}^{d-1} \binom{r}{j}. \tag{5}$$

Equivalently,

$$\beta_r(d) \leq \sum_{j=0}^{d} \binom{r}{j}. \tag{6}$$

In Section 6, two proofs of Theorem 4 are given. Elaborating on one of them, we will also establish the following slight refinement.

Theorem 4′. *For integer $r \geq d \geq 0$ we have*

$$(1 - 2^{d-r})\beta_r(d) \leq \sum_{j=0}^{d} \binom{r}{j} - 2^d.$$

It is not difficult to derive from Theorem 4′, for instance, that $\beta_r(d) \leq \sum_{j=0}^{d}\binom{r}{j} - 2^{d-1}$ whenever $d < r/2$, or that $\beta_r(d) \leq \sum_{j=0}^{d}\binom{r}{j} - 2^d$ whenever $d < 0.227r$ (for the latter conclusion assume, for a contradiction, that $\beta_r(d) \geq \sum_{j=0}^{d}\binom{r}{j} - 2^d + 1$, and use (4)).

5. Constructions: upper bounds for γ_r, lower bounds for β_r

All bounds listed in this section are constructive. We confine here to the resulting estimates and comparison between them, with the underpinning constructions being incorporated into the proofs (presented in Section 7). For the background material in coding theory (simplex codes, dual-BCH codes, Greismer and Carlitz-Uchiyama bounds), the reader can refer any standard textbook, such as [McWS77, vL98].

Theorem 5. *For any integer $r \ge d \ge 3$ we have*

$$\gamma_r(d) < K_d \cdot 2^{\left(\frac{1}{2}-\varepsilon_d\right)r},$$

where $\varepsilon_d = \frac{1}{2(2^d-1)}$ and $K_d = (2^d-1)2^{2^{d-1}-(3/2)+\varepsilon_d}$.

As a particular case to be compared against Theorem 3, we have $\gamma_r(3) = O(2^{3r/7})$.

As the reader will see, the proof of Theorem 5 relies on the properties of simplex codes. The reason to prefer simplex codes over other codes is that these codes have the largest possible relative minimum distance among all codes of given dimension d (as the Griesmer bound readily shows). The drawback of the simplex codes, on the other hand, is that their length is exponential in the dimension, leading eventually to the double-exponential dependence on d in the constant K_d of Theorem 5, and hence resulting in very poor bounds as d grows. Indeed, the estimate of the theorem becomes trivial for $d \sim \log r$. Using other codes one can produce non-trivial estimates for reasonably large values of d. Specifically, the argument employed in the proof of Theorem 5 shows that if n and μ are positive integers such that there exists a code S of length n, minimum distance μ, dimension d, and the largest weight M satisfying $(n-M)\lfloor r/n \rfloor \ge d$, then

$$\gamma_r(d) < 2^{(1-\mu/n)r+n+d-\mu}.$$

Indeed, it suffices that the dimension of S be *at least* d, as it follows by considering any subcode of S of dimension d. Choosing S to be the dual of a BCH code with appropriately chosen parameters, we prove

Theorem 6. *There exists an absolute constant K such that for any integer $r \ge d \ge 3$ we have*

$$\gamma_r(d) < 2^{0.5r+K(dr/\log_2 r)^{2/3}}.$$

Hence, if $d = o(\sqrt{r}\log_2 r)$, then $\gamma_r(d) < 2^{(0.5+o(1))r}$.

We now turn to estimates which (unlike those of Theorems 5 and 6) are mostly of interest for flats of low *co*-dimension.

Theorem 7. *For integer r and d with $2 \le d \le r/2$, let ρ denote the remainder of the division of r by $2d$. Then*

$$\beta_r(d) = \sum_{\substack{0\le i\le 2d-\rho,\, 0\le j\le \rho \\ i+j=d}} \binom{2d-\rho}{i}\binom{\rho}{j} \left\lfloor \frac{r}{2d} \right\rfloor^i \left(\left\lfloor \frac{r}{2d} \right\rfloor + 1\right)^j$$

Consequently,

$$\beta_r(d) \ge \binom{2d}{d} \left\lfloor \frac{r}{2d} \right\rfloor^d.$$

We notice that Theorems 4 and 7 give $\beta_r(d) = \Omega_d(r^d)$. It follows, say, that $\gamma_r(r-2) = 2^r - \Omega(r^2)$; compared with Theorem 2 this shows that γ_r, considered as a function of $d \in [0, r]$, exhibits a highly asymmetric behavior.

Theorem 8. *For integer $r \ge d \ge 2$, let ρ denote the remainder of the division of r by d. Then*

$$\beta_r(d) \ge \left(\left\lfloor \frac{r}{d} \right\rfloor + 1\right)^{d-\rho} \left(\left\lfloor \frac{r}{d} \right\rfloor + 2\right)^{\rho}.$$

Consequently,

$$\beta_r(d) > (r/d)^d,$$

and if $d \ge r/2$, then

$$\beta_r(d) \ge \left(\frac{3}{2}\right)^r \left(\frac{4}{3}\right)^d.$$

While the bounds of Theorems 7 and 8 may not be easy to compare analytically, computations suggest that Theorem 7 gives a better estimate for all $d \le r/2$, save for a finite (and small) number of exceptional pairs (d, r). For $d > r/2$ Theorem 7 yields

$$\beta_r(d) \ge \beta_r(\lfloor r/2 \rfloor) \ge \binom{2\lfloor r/2 \rfloor}{\lfloor r/2 \rfloor}, \tag{7}$$

which is superseded by Theorem 8 for d very close to r; namely, for $r - d \lesssim 1.738 \ln r$. We also notice that if, indeed, $r - d \lesssim 1.443 \ln r$, then Theorem 8 itself is superseded by Theorem 5.

Theorem 9. *Suppose that $r \ge d \ge 1$, $k \ge 1$, and $r_i \ge d_i \ge 0$ $(i = 1, \dots, k)$ are integers such that $r_1 + \dots + r_k \le r$, $d_1 + \dots + d_k \le d$, and $r_i \le d + d_i$ for $i = 1, \dots, k$. Then*

$$\beta_r(d) \ge \binom{r_1}{d_1} \cdots \binom{r_k}{d_k}.$$

It is not difficult to see that for $d \ge r/2$, Theorem 9 gives

$$\beta_r(d) \ge \binom{r}{\lfloor r/2 \rfloor};$$

this is identical or marginally stronger than (7). For $1 \le d \le r/2$, the maximum of the product $\binom{r_1}{d_1} \cdots \binom{r_k}{d_k}$ under the constrains $r_i \ge d_i \ge 0$, $r_1 + \cdots + r_k \le r$, and $d_1 + \cdots + d_k \le d$ (with $r_i \le d + d_i$ *not* assumed!) is $\binom{r}{d}$; this is to be compared with Theorem 4 and also with the following corollary.

Corollary 2. *If $r \ge 1$ and $\sqrt{r} < d \le r/2$ are integer, then*

$$\beta_r(d) > e^{rH(d/r) - 2(r/d)\ln r}.$$

Consequently, if $d/\sqrt{r} \to \infty$ and $d \le r/2$, then

$$\beta_r(d) > \binom{r}{d}^{1+o(1)}.$$

A precise comparison between Theorems 7 and 9 is hardly feasible. However, the "main terms" (cf. Corollary 2) are easy to compare, and it turns out that

$$e^{rH(d/r)} > \binom{2d}{d} \left(\frac{r}{2d}\right)^d$$

for all positive integer r and $d \le r/2$. We remark, on the other hand, that Theorem 9 fails to produce reasonable bounds if d is very small (as compared to r).

6. Proofs, I: non-existence results

Proof of Theorem 3. Suppose that $C \subseteq \mathbb{F}_2^r$ is 3-complete; that is, every element $v \in \mathbb{F}_2^r$ lies in a 3-flat F_v with the other seven elements in C. We want to show that if $r \ge 15$, then $|C| > c \cdot 2^{3r/8}$.

Let S be the set of all those $s \in \mathbb{F}_2^r$ representable as a sum of two distinct elements of C, and for each $s \in S$ denote by $\nu(s)$ the number of such representations, with two representations that differ by the order of summands considered identical. Write $B := \mathbb{F}_2^r \setminus C$, and for each $s \in S$ let $B(s)$ be the set of all those $b \in B$ with $s \in b + F_b$. (Notice, that $b + F_b$ is the linear 3-subspace, parallel to the flat F_b.) Thus, every $b \in B$ belongs to exactly seven sets $B(s)$, and hence

$$\sum_{s \in S} |B(s)| = 7|B|. \tag{8}$$

For every $s \in S$ and $b \in B(s)$ there are three distinct representations $s = c_1 + c_2$ with $c_1, c_2 \in F_b \cap C$. Since these representations uniquely determine F_b, and hence b itself, we

have

$$|B(s)| \le \binom{\nu(s)}{3} < \frac{1}{6}\,(\nu(s))^3. \tag{9}$$

Also,

$$|B(s)| \le |C| \tag{10}$$

as $b + s \in F_b \setminus \{b\}$ for each $b \in B(s)$, implying $B(s) + s \subseteq C$.

Averaging multiplicatively (9) and (10) with the exponent weights 1/3 and 2/3, respectively, we get

$$|B(s)| < \frac{1}{\sqrt[3]{6}}\,|C|^{2/3}\nu(s),$$

and substitution into (8) yields

$$7(2^r - |C|) < \frac{1}{\sqrt[3]{6}}\,|C|^{2/3}\sum_{s\in S}\nu(s) = \frac{1}{\sqrt[3]{6}}\,|C|^{2/3}\binom{|C|}{2}. \tag{11}$$

If $|C| \ge 2^{r/2}$, then we are done as $2^{r/2} > c \cdot 2^{3r/8}$ for $r \ge 15$. If $|C| < 2^{r/2}$, then $(2^r - |C|)/(|C| - 1) > 2^r/|C|$; consequently, (11) gives

$$|C|^{8/3} > 14\sqrt[3]{6} \cdot 2^r$$

implying the result. □

Next, we give two proofs of Theorem 4. Both proofs rely on the fact that if $\mathcal{L}_{r,d}$ is the vector space of all multilinear polynomials in r variables over the field $\mathbb{F}_2$ of total degree at most d, then $\dim \mathcal{L}_{r,d} = \sum_{j=0}^{d}\binom{r}{j}$ (which is immediate from looking at the "monomial basis"). Nevertheless, the two proofs seem to differ significantly. We keep using the notation $\mathcal{L}_{r,d}$ below.

Our first proof goes along the lines of Dvir's proof [D09] of the finite field Kakeya conjecture. We need two basic facts about polynomials over the field $\mathbb{F}_2$.

Fact 1. For integer $d \ge 1$, a polynomial in d variables over $\mathbb{F}_2$ of degree smaller than d cannot vanish on all, but at most one point of $\mathbb{F}_2^d$. (To see this, observe that every monomial of the polynomial in question is independent of at least one variable, hence the sum of its values over $\mathbb{F}_2^d$ is equal to 0.)

Fact 2. For integer $r \ge 1$, a non-zero multilinear polynomial in r variables over $\mathbb{F}_2$ cannot vanish on all points of $\mathbb{F}_2^r$. (For the proof, notice that every function from $\mathbb{F}_2^r$ to $\mathbb{F}_2$ can be represented by a multilinear polynomial, and that both the total number of all functions and the total number of all multilinear polynomials are equal to 2^{2^r}. Thus, every function is *uniquely* represented by such a polynomial.)

First proof of Theorem 4. Assuming that (5) is false, find a d-complete set $C \subseteq \mathbb{F}_2^r$ with $|C| < \sum_{j=0}^{d-1} \binom{r}{j}$. Thus, for every $v \in \mathbb{F}_2^r$ there exists a d-subspace $L_v \le \mathbb{F}_2^r$ with $v + (L_v \setminus \{0\}) \subseteq C$. Since $\dim \mathcal{L}_{r,d-1} = \sum_{j=0}^{d-1} \binom{r}{j}$, the evaluation map from $\mathcal{L}_{r,d-1}$ to $\mathbb{F}_2^{|C|}$ (sending every polynomial to the $|C|$-tuple of its values at the points of C) is degenerate. Hence, there is a non-zero polynomial $P \in \mathcal{L}_{r,d-1}$ vanishing at every point of C. As a result, for each $v \in \mathbb{F}_2^r$ there exist $v_1, \dots, v_d \in \mathbb{F}_2^r$ such that

$$P(v + t_1 v_1 + \dots + t_d v_d) = 0, \quad (t_1, \dots, t_d) \in \mathbb{F}_2^d \setminus \{0\}.$$

This means that the polynomial

$$P(v + T_1 v_1 + \dots + T_d v_d) \in \mathbb{F}_2[T_1, \dots, T_d]$$

vanishes at every point of $\mathbb{F}_2^d \setminus \{0\}$. The degree of this polynomial is at most $\deg P \le d-1$. Hence, by Fact 1, we have $P(v) = 0$; that is, P vanishes at every point of $\mathbb{F}_2^r$. This, however, contradicts Fact 2. □

Second proof of Theorem 4. Aiming at (6), fix $B \subseteq \mathbb{F}_2^r$ with $|B| = \beta_r(d)$ such that to every $b \in B$ there corresponds a co-d-flat $F_b \subseteq \mathbb{F}_2^r$ with $F_b \cap B = \{b\}$. For every such flat, find a polynomial $P_b \in \mathcal{L}_{r,d}$ with $P_b(z) = 1$ whenever $z \in F_b$, and $P_b(z) = 0$ otherwise. (Such a polynomial can be constructed by taking the product of d linear factors corresponding to d hyperplanes whose intersection is F_b.) These $|B|$ polynomials are linearly independent, as it follows by substituting the points $b \in B$ into their linear combinations. Consequently,

$$\beta_r(d) = |B| \le \dim \mathcal{L}_{r,d} = \sum_{j=0}^{d} \binom{r}{j}.$$

□

Proof of Theorem 4′. We elaborate on the second proof of Theorem 4. Fix a d-non-blocking set $B \subseteq \mathbb{F}_2^r$ with $|B| = \beta_r(d)$, and write $C := \mathbb{F}_2^r \setminus B$. For each $v \in \mathbb{F}_2^r$ find a co-d-flat F_v with $v \in F_v \subseteq C \cup \{v\}$ and, as above, let $P_v \in \mathcal{L}_{r,d}$ be an "indicator polynomial" of F_v. Write $\mathcal{P}_B := \{P_b \colon b \in B\}$ and $\mathcal{P}_C := \{P_c \colon c \in C\}$. Notice, that the subspace of $\mathcal{L}_{r,d}$ generated by $\mathcal{P}_B$ intersects trivially the subspace generated by $\mathcal{P}_C$: for if

$$\sum_{b \in B} \varepsilon(b) P_b = \sum_{c \in C} \varepsilon(c) P_c$$

with $\varepsilon \colon \mathbb{F}_2^r \to \mathbb{F}_2$ then, evaluating at any specific $b \in B$, we get $\varepsilon(b) = 0$. Thus, denoting by L_C the subspace, generated by $\mathcal{P}_C$, we have

$$|B| \le \dim \mathcal{L}_{r,d} - \dim L_C,$$

and we claim that $\dim L_C \geq 2^{-(r-d)}|C|$. To see this, we observe that for any subset $C_0 \subseteq C$ with $|C_0| < 2^{-(r-d)}|C|$, we have

$$\left|\bigcup_{c\in C_0} F_c\right| \leq 2^{r-d} \cdot |C_0| < |C|,$$

and that for any $c' \notin \cup_{c\in C_0} F_c$, the polynomial $P_{c'}$ is not a linear combination of the polynomials P_c with $c \in C_0$. Consequently, we have

$$|B| \leq \dim \mathcal{L}_{r,d} - 2^{-(r-d)}|C| = \dim \mathcal{L}_{r,d} - 2^{-(r-d)}(2^r - |B|),$$

whence

$$(1 - 2^{d-r})|B| \leq \sum_{j=0}^{d} \binom{r}{j} - 2^d$$

implying the result. □

7. Proofs, II: constructions

Proof of Theorem 5. For $r < 2^d - 1$ the assertion follows, by a straightforward computation, from the trivial estimate $\gamma_r(d) < 2^r$. Suppose, therefore, that $r \geq 2^d - 1$.

Write $n := 2^d - 1$ and let $S < \mathbb{F}_2^n$ be the simplex code of length n. Thus, S is a d-subspace of $\mathbb{F}_2^n$, generated by the rows of the $d \times n$ matrix whose columns are all the non-zero vectors in $\mathbb{F}_2^d$, and every non-zero element of S has weight 2^{d-1} with respect to the standard basis of $\mathbb{F}_2^n$. Choose subspaces $V_1, \ldots, V_n \leq \mathbb{F}_2^r$ so that $\mathbb{F}_2^r = V_1 \oplus \cdots \oplus V_n$ and the dimension of each V_i is either $\lfloor r/n \rfloor$ or $\lceil r/n \rceil$, and consider the set

$$C := \bigcup_{(s_1,\ldots,s_n)\in S\setminus\{0\}} \quad \bigoplus_{i\in[1,n]\colon s_i=0} V_i.$$

We have

$$\begin{aligned} |C| &< \sum_{c\in S\setminus\{0\}} 2^{(n-2^{d-1})\lceil r/n\rceil} \\ &\leq (2^d - 1)\, 2^{(2^{d-1}-1)\left(\frac{r-1}{n}+1\right)} \\ &= K_d \cdot 2^{\left(\frac{1}{2}-\varepsilon_d\right)r}, \end{aligned}$$

and to complete the proof we show that for every $v \in \mathbb{F}_2^r$ there is a d-flat passing through v and contained in $C \cup \{v\}$. To this end, we write $v = v_1 + \cdots + v_n$ with $v_i \in V_i$ for $= 1, \ldots, n$, and let

$$\begin{aligned} F_v &:= \left\{\sum\nolimits_{i\in[1,n]\colon s_i=0} v_i \colon (s_1, \ldots, s_n) \in S\right\} \\ &= v + \{s_1 v_1 + \cdots + s_n v_n \colon (s_1, \ldots, s_n) \in S\}. \end{aligned}$$

Evidently, F_v is a flat with $v \in F_v \subseteq C \cup \{v\}$. Moreover, the dimension of F_v is at most d. If it is equal to d, then we are done. Otherwise, there exists an element

$(s_1,\dots,s_n)\in S\setminus\{0\}$ such that $s_1v_1+\dots+s_nv_n=0$; equivalently, v is an element of the subspace $\oplus_{i\in[1,n]\colon s_i=0}V_i\subseteq C$, and we conclude the proof observing that the dimension of this subspace is at least $(2^{d-1}-1)\lfloor r/n\rfloor\ge d$. □

As we have mentioned in Section 5 (and the reader can easily check now), the argument employed in the proof of Theorem 5 shows that if n and μ are positive integers such that there exists a code S of length n, minimum distance μ, dimension at least d, and the largest weight M satisfying $(n-M)\lfloor r/n\rfloor\ge d$, then

$$\gamma_r(d)<2^{(1-\mu/n)r+n+d-\mu}. \tag{12}$$

This observation is used in the proof of Theorem 6 below.

Proof of Theorem 6. Consider the code dual to the BCH code with the parameters m and e defined by

$$m:=\left\lceil\frac{2}{3}\left(\log_2(dr)-\log_2\log_2(dr)\right)\right\rceil,\ e:=\left\lceil\frac{d}{m}\right\rceil.$$

This is a code of length $n:=2^m-1$, with the weight of every non-zero code word in the interval $[0.5n-(e-1)\sqrt{n},0.5n+(e-1)\sqrt{n}\,]$ and consequently, having the minimum distance

$$\mu\ge 0.5n-(e-1)\sqrt{n}$$

and the maximum distance

$$M\le 0.5n+(e-1)\sqrt{n}$$

(the Carlitz-Uchiyama bound).

We notice that $r\ge d\ge 3$ implies $rd\ge 9$, whence

$$m\ge 0.25\log_2(dr). \tag{13}$$

Also,

$$\frac{1}{2}\left(\frac{dr}{\log_2(dr)}\right)^{2/3}\le n<2\left(\frac{dr}{\log_2(dr)}\right)^{2/3} \tag{14}$$

(the first inequality following from $n=2^m-1\ge 2^{m-1}$).

Assuming now

$$d<c\sqrt{r}\log_2 r \tag{15}$$

with a sufficiently small absolute constant $c>0$ (as we clearly can, choosing K large enough), by (14) we get

$$r>c^{-2/3}\left(\frac{dr}{\log_2(dr)}\right)^{2/3}>n \tag{16}$$

and, by (14), (15), and (13),

$$\frac{e-1}{\sqrt{n}} < \frac{d}{m\sqrt{n}} < 2\frac{d}{m}\left(\frac{\log_2(dr)}{dr}\right)^{1/3} < 2c^{2/3}\,\frac{\log_2(dr)}{m} < 0.25.$$

As a result, and taking into account (16) and (15),

$$(n-M)\,\lfloor r/n\rfloor > (0.5n-(e-1)\sqrt{n})\frac{r}{2n} > 0.125r > d.$$

Furthermore, a straightforward computation confirms that (15) yields $e \le 2^{\lceil m/2\rceil-1}$, which is known to imply that the dimension of the code under consideration is $em \ge d$. The result now follows by applying (12) and observing that, by (14) and (13),

$$\frac{dr}{m\sqrt{n}} = \frac{n}{m}\frac{dr}{n^{3/2}} < 3n\frac{\log_2(dr)}{m} \le 12n,$$

whence

$$\begin{aligned}\left(1-\frac{\mu}{n}\right)r+n+d-\mu &< \left(1-\frac{\mu}{n}\right)r+2n\\ &\le \left(0.5+\frac{e-1}{\sqrt{n}}\right)r+2n\\ &< 0.5r+\left(\frac{dr}{m\sqrt{n}}+2n\right)\\ &< 0.5r+14n.\end{aligned}$$

□

Proof of Theorem 7. Observing that

$$(2d-\rho)\left\lfloor\frac{r}{2d}\right\rfloor+\rho\left(\left\lfloor\frac{r}{2d}\right\rfloor+1\right)=\left\lfloor\frac{r}{2d}\right\rfloor\cdot 2d+\rho=r,$$

choose subspaces $V_1,\dots,V_{2d}\le\mathbb{F}_2^r$ with $\mathbb{F}_2^r=V_1\oplus\cdots\oplus V_{2d}$ so that

$$\dim V_1=\cdots=\dim V_{2d-\rho}=\left\lfloor\frac{r}{2d}\right\rfloor$$

and

$$\dim V_{2d-\rho+1}=\cdots=\dim V_{2d}=\left\lfloor\frac{r}{2d}\right\rfloor+1.$$

In every subspace V_i fix a basis $\mathfrak{e}_i$. For $v\in\mathbb{F}_2^r$ let $\operatorname{supp} v$ denote the support of v with respect to the union of the bases $\mathfrak{e}_i$, and for each $i\in[1,2d]$ let $\operatorname{supp}_i(v):=\operatorname{supp}(v)\cap\mathfrak{e}_i$. Also, let $w(v)=|\operatorname{supp}(v)|$ and $w_i(v):=\operatorname{supp}_i(v)$; that is, $w(v)$ is the weight of v with respect to the union of the bases $\mathfrak{e}_i$, and $w_i(v)$ is the contribution of $\mathfrak{e}_i$ to $w(v)$, so that $w=w_1+\cdots+w_{2d}$. Finally, set

$$B:=\{v\in\mathbb{F}_2^r\colon w(v)=d \text{ and } w_1(v),\dots,w_{2d}(v)\le 1\};$$

thus,

$$|B| = \sum_{\substack{0\le i\le 2d-\rho,\, 0\le j\le \rho\\ i+j=d}} \binom{2d-\rho}{i}\binom{\rho}{j} \left\lfloor \frac{r}{2d}\right\rfloor^i \left(\left\lfloor \frac{r}{2d}\right\rfloor + 1\right)^j,$$

and we show that through every $v \in \mathbb{F}_2^r$ passes a flat F_v of co-dimension at most d, disjoint with $B \setminus \{v\}$. We distinguish three cases.

If $v \in B$, then we let

$$F_v := \{u \in \mathbb{F}_2^r \colon \operatorname{supp} v \subseteq \operatorname{supp} u\}.$$

Evidently, we have $v \in F_v$ and $\operatorname{codim} F_v = w(v) = d$; moreover, if $u \in F_v \setminus \{v\}$, then $w(u) > w(v) = d$, implying $u \notin B$.

If there exists $i \in [1, 2d]$ with $w_i(v) \ge 2$, then we choose $E \subseteq \operatorname{supp}_i(v)$ with $|E| = 2$ and set

$$F_v := \{u \in \mathbb{F}_2^r \colon E \subseteq \operatorname{supp}(u)\}.$$

We have $v \in F_v,\ F_v \cap B = \varnothing$, and $\operatorname{codim} F_v = 2$.

Finally, if $v \notin B$ and $w_i(v) \le 1$ for each $i \in [1, 2d]$, then there exists $I \subseteq [1, 2d]$ with $|I| = d + 1$ such that for all $i \in I$, the weights $w_i(v)$ are equal to each other. In this case we take F_v to be the co-d-flat (actually, a co-d-subspace) consisting of those $u \in \mathbb{F}_2^r$ with the property that for all $i \in I$, the weights $w_i(u)$ are of the same parity. It is immediately verified that $v \in F_v$ and $F_v \cap B = \varnothing$. □

Proof of Theorem 8. Choose subspaces $V_1, \dots, V_d \le \mathbb{F}_r$ with $\mathbb{F}_2^r = V_1 \oplus \dots \oplus V_d$ so that

$$\dim V_1 = \dots = \dim V_{d-\rho} = \left\lfloor \frac{r}{d}\right\rfloor$$

and

$$\dim V_{d-\rho+1} = \dots = \dim V_d = \left\lfloor \frac{r}{d}\right\rfloor + 1.$$

In every subspace V_i fix a basis $\mathfrak{e}_i$, and define the sets supp, supp_i, and the weight functions w and w_i as in the proof of Theorem 7. Let

$$B := \{v \in \mathbb{F}_2^r \colon w_i(v) \le 1,\ i \in [1, d]\};$$

thus,

$$|B| = \left(\left\lfloor \frac{r}{d}\right\rfloor + 1\right)^{d-\rho} \left(\left\lfloor \frac{r}{d}\right\rfloor + 2\right)^{\rho},$$

and we claim that through every $v \in \mathbb{F}_2^r$ passes a flat F_v of co-dimension at most d, disjoint with $B \setminus \{v\}$. To show this we distinguish two cases, according to whether $v \in B$ or $v \notin B$.

If there exists $i \in [1,d]$ with $w_i(v) > 1$ (that is, $v \notin B$), then we choose $E \subseteq \operatorname{supp}_i(v)$ with $|E| = 2$, and set

$$F_v := \{u \in \mathbb{F}_2^r \colon E \subseteq \operatorname{supp}(u)\}.$$

Clearly, this is a flat of co-dimension 2, disjoint with B and passing through v.

If, on the other hand, we have $w_i(v) \le 1$ for each $i \in [1,d]$ (that is, $v \in B$), then we consider the partition $[1,d] = I_0 \cup I_1$ with

$$I_\nu := \{i \in [1,d] \colon w_i(v) = \nu\}; \quad \nu \in \{0,1\}$$

and let F_v be the co-d-flat consisting of those vectors $u \in \mathbb{F}_2^r$ with the property that $w_i(u)$ is even for each $i \in I_0$, and $\operatorname{supp}_i v \subseteq \operatorname{supp}_i u$ for each $i \in I_1$. It is immediately verified that $F_v \cap B = \{v\}$. □

Proof of Theorem 9. Letting $K := r - (r_1 + \cdots + r_k)$, $r_{k+1} = \cdots = r_{k+K} = 1$, and $d_{k+1} = \cdots = d_{k+K} = 0$, we see that $r_1 + \cdots + r_k = r$ can be assumed without loss of generality. With this extra assumption, we choose subspaces $V_1, \dots, V_k \le \mathbb{F}_2^r$ so that $\mathbb{F}_2^r = V_1 \oplus \cdots \oplus V_k$ and $\dim V_i = r_i$ for $i = 1, \dots, k$, in every subspace V_i fix a basis $\mathfrak{e}_i$, and define supp, supp_i, w, and w_i as in the proofs of Theorems 7 and 8. Finally, we set

$$B := \{v \in \mathbb{F}_2^r \colon w_i(v) = d_i,\ i \in [1,k]\};$$

thus,

$$|B| = \binom{r_1}{d_1} \cdots \binom{r_k}{d_k},$$

and we claim that through every $v \in \mathbb{F}_2^r$ passes a flat F_v of co-dimension at most d, disjoint with $B \setminus \{v\}$. To show this we distinguish several cases: the case where $v \in B$, that where $w_i(v) \ge d_i + 1$ for some $i \in [1,k]$, and that where $w_i(v) \le d_i - 1$ for some $i \in [1,k]$, with the last two cases further splitting into two subcases each.

If $v \in B$, then we take $F_v := \{u \in \mathbb{F}_2^r \colon \operatorname{supp} v \subseteq \operatorname{supp} u\}$. Clearly, $F_v \cap B = \{v\}$, and the co-dimension of F_v is $d_1 + \cdots + d_k \le d$.

If there exists $i \in [1,k]$ with $w_i(v) \ge d_i + 1$, then we find $E \subseteq \operatorname{supp}_i(v)$ with $|E| = d_i + 1$, and set

$$F_v := \{u \in \mathbb{F}_2^r \colon E \subseteq \operatorname{supp}(u)\} \quad \text{if } d_i < d,$$

and

$$F_v := \{u \in \mathbb{F}_2^r \colon E \subseteq \operatorname{supp}(u) \text{ or } E \cap \operatorname{supp}(u) = \varnothing\} \quad \text{if } d_i = d.$$

Clearly, we have $v \in F_v$, and

$$\operatorname{codim} F_v = \begin{cases} |E| = d_i + 1 \le d & \text{if } d_i < d, \\ |E| - 1 = d_i = d & \text{if } d_i = d. \end{cases}$$

Furthermore, we have $F_v \cap B = \varnothing$: for, if $E \subseteq \operatorname{supp}(u)$, then $w_i(u) \ge |E| > d_i$, and if $E \cap \operatorname{supp}(u) = \varnothing$ and $d_i = d$, then

$$w_i(u) \le r_i - |E| \le (d_i + d) - (d_i + 1) < d = d_i.$$

In a similar way we treat the situation where $w_i(v) \le d_i - 1$ for some $i \in [1, k]$. In this case we find a set $E \subseteq \mathfrak{e}_i \setminus \operatorname{supp}_i(v)$ with $|E| = r_i - d_i + 1$, and let

$$F_v := \{u \in \mathbb{F}_2^r \colon E \cap \operatorname{supp}(u) = \varnothing\} \quad \text{if } r_i < d_i + d,$$

and

$$F_v := \{u \in \mathbb{F}_2^r \colon E \cap \operatorname{supp}(u) = \varnothing \text{ or } E \subseteq \operatorname{supp}(u)\} \quad \text{if } r_i = d_i + d.$$

Thus, $v \in F_v$, the co-dimension of F_v is

$$\operatorname{codim} F_v = \begin{cases} |E| = r_i - d_i + 1 \le d & \text{if } r_i < d_i + d, \\ |E| - 1 = r_i - d_i = d & \text{if } r_i = d_i + d, \end{cases}$$

and F_v is disjoint with B: for, if $\operatorname{supp}(u) \cap E = \varnothing$, then $w_i(u) \le r_i - |E| = d_i - 1 < d_i$, and if $E \subseteq \operatorname{supp}(u)$ and $r_i = d_i + d$, then $w_i(u) \ge |E| = d + 1 > d_i$, implying $u \notin B$ in both cases. □

Proof of Corollary 2. Let

$$k := \left\lfloor \frac{r}{d} \right\rfloor, \ d_1 := \left\lfloor \frac{d}{k} \right\rfloor, \text{ and } \ r_1 := \left\lfloor \frac{d_1}{d}\, r \right\rfloor;$$

thus,

$$2 \le k < d \tag{17}$$

(as $2 \le \frac{r}{d} < d$), and

$$\frac{d}{r} \le \frac{d_1}{r_1} \le \frac{1}{2} \tag{18}$$

(the first inequality following from $r_1 \le \frac{d_1}{d}\, r$, the second from $\frac{d_1}{d}\, r \ge 2d_1$). Observing also that

$$kd_1 \le d, \ kr_1 \le kd_1 \frac{r}{d} \le r,$$

and

$$r_1 - d_1 = \left\lfloor \left(\frac{r}{d} - 1 \right) d_1 \right\rfloor \le kd_1 \le d,$$

we apply Theorem 9 with $r_2 = \cdots = r_k = r_1$ and $d_2 = \cdots = d_k = d_1$ to get

$$\beta_r(d) \geq \binom{r_1}{d_1}^k.$$

Consequently, (4) yields

$$\ln \beta_r(d) \geq k r_1 H(d_1/r_1) - (k/2)\ln(2r_1). \tag{19}$$

Now from

$$r_1 + k \geq \left\lfloor \frac{r}{d} + \frac{d_1}{d}\, r \right\rfloor - 1 = \left\lfloor (d_1+1)\frac{r}{d} \right\rfloor - 1 \geq \left\lfloor \frac{d+1}{k}\,\frac{r}{d} \right\rfloor - 1$$
$$= \left\lfloor \frac{r}{k} + \frac{r}{kd} \right\rfloor - 1 > \frac{r}{k} + \frac{r}{kd} - 2 \geq \frac{r}{k} - 1$$

and (17) we deduce

$$k r_1 > r - k^2 - k \geq r - (3/2)k^2,$$

from (18) and the fact that H is increasing on $[0, 1/2]$ we conclude that

$$H(d_1/r_1) \geq H(d/r),$$

and $r_1 \leq \frac{d_1}{d}\, r \leq \frac{r}{k}$ along with (17) gives $2r_1 \leq r$. Combining these observations with (19) we obtain

$$\ln \beta_r(d) > (r - (3/2)k^2) H(d/r) - (k/2)\ln r.$$

To derive the first assertion of the corollary we now notice that the inequality

$$H(t) \leq t \ln(e/t),\ t \in [0,1]$$

gives

$$(3/2)k^2 H(d/r) + (k/2)\ln r \leq \frac{3}{2}\,\frac{r}{d}\ln\frac{er}{d} + \frac{1}{2}\,\frac{r}{d}\ln r < 2\frac{r}{d}\ln r$$

since $d \geq 3$ by (17). For the second assertion just observe that if $d/\sqrt{r} \to \infty$, then $rH(d/r) \geq d \ln \frac{r}{d}$ whereas $\frac{r}{d}\ln r = o(d \ln \frac{r}{d})$, and use (4). □

References

[CHLL97] G. Cohen, I. Honkala, S. Litsyn, and A. Lobstein, *Covering codes*. North-Holland Mathematical Library **54**. North-Holland Publishing Co., Amsterdam, 1997.

[D09] Z. Dvir, On the size of Kakeya sets in finite fields, *J. Amer. Math. Soc.* **22** (4) (2009), 1093–1097.

[McWS77] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland (1977).

[vL98] J.H. van Lint, *An Introduction to Coding Theory*, Third edition, Springer Verlag (1998).

E-mail address: A.Blokhuis@tue.nl

Department of Mathematics and Computer Science, Eindhoven University of Technology, Netherlands

E-mail address: seva@math.haifa.ac.il

Department of Mathematics, The University of Haifa at Oranim, Israel